Elimination of Social Security Numbers for Identification within the Department of Defense

Subject Area Topical Issues

EWS 2006

Elimination of Social Security Numbers for Identification within the Department of Defense

EWS Contemporary Issues Paper
Submitted by Captain ME Cover
to
Major SA Uecker, CG #7
February 2005

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **FEB 2005**	2. REPORT TYPE	3. DATES COVERED **00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE
Elimination of Social Security Numbers for Identification Within the Department of Defense

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Marine Corps University Library ,2040 Broadway Street ,Quantico,VA,22134

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**14**	

Identity theft affects approximately ten million Americans each year[1] and costs consumers and businesses more than $53 billion in losses.[2] In a 2003 study conducted by the Identity Theft Resource Center, fraudulent charges were reported to average more the $90,000 per name used, and the average time spent by victims trying to correct their credit standing was approximately 600 hours.[3] The widespread use of social security numbers (SSN) as a means of individual identification and the compromise of that information, has significantly contributed to the rise in cases of identity theft.

Current Department of Defense (DoD) strategies aimed at protecting service members from identity theft are inadequate because they do not address the fundamental vulnerability represented by the use of SSNs as service member identification numbers.

[1] "Identity Theft Focus of National Consumer Protection Week 2005," *For the Consumer, Federal Trade Commission,* 7 February 2005, <http://www.ftc.gov/opa/2005/02/ncpw05.htm> (14 November 2005).

[2] Mitch Swanda, "Protecting Your Personal Top Secret," *National Military Family Association,* January 2005, <http://www.nmfa.org/site/PageServer?pagename=usaa_article_id_theft> (14 November 2005).

[3] Linda Foley and Jay Foley, "Identity Theft: The Impact 2003. A Comprehensive Study to Understand the Impact of Identity Theft on Known Victims," *Identity Theft Resource Center,* 2003, <http://idtheftcenter.com/idaftermath.pdf> (14 November 2005).

Affected Service Members

The Naval Inspector General’s office defines identity theft as “the illegal, fraudulent use of your name, date of birth, and [or] Social Security Number and other identifying information unique to you, used by another individual in order to obtain goods, services, merchandise, cash, or property.”[4] In fact, this crime has been made far more insidious as a result of the profound growth of the Internet and the generally unrestricted flow of information that it symbolizes.

Identity theft can represent a unique burden to service members particularly in a deployed environment or while collecting a fixed retirement income. Consider the case of retired Army Captain John Harrison. In July of 2001, two years after Harrison’s retirement, a man named Jerry Wayne Philips walked into a military identification card processing office with Harrison’s SSN and was able to walk out with a valid military identification card. By the time he was caught on 12 December 2001, Phillips had accumulated $260,000 in debts under Harrison’s name. He also opened four checking and two savings accounts, purchased motorcycles and trucks, and even established a time-share in Hilton Head, South Carolina, and a beach rental

[4] “Identity Theft – What It Is And How To Avoid It (LAPA 01-04),” *Naval Inspector General*, <http://www.ig.navy.mil/Intelligence%20and%20Security%20(Identity%20Theft).htm> (14 November 2005).

home in Virginia. As of late 2004, Harrison was still trying to clear his credit standing that at one time included garnishment of his retirement pay and demands from the Internal Revenue Service (IRS) for payment of back taxes not legitimately owed.[5] While the use of a fraudulent military identification card for purposes of engaging in identity theft is not a common occurrence, this example does serve to highlight the vulnerabilities that exist.

Navy Commander Frank Mellott was also a victim of identity theft. An estranged half-brother initially used Mellot's SSN as a means of avoiding payment of child support but expanded its use to include opening cable television and wireless telephone services. In addition to the damage to his personal credit rating, Mellott was also in danger of losing his Top Secret security clearance that would have adversely impacted his seventeen-year naval career.[6]

The adversity experienced by both of these men was significant; however, it is not difficult to imagine how much more complicated each scenario would have been if the service

[5] Laura Bruce, "John Harrison – The Face of Identity Theft," *Bankrate.com,* 18 August 2004. <http://www.bankrate.com/brm/news/advice/IDTheft/ID-home.asp> (14 November 2005).

[6] Donna Miles, "Military Takes Steps Against Identity Theft," *Military Money.* Winter 2004-2005. <http://www.militarymoney.com/money/1101916428> (15 November 2005).

members had been deployed in a combat zone with little or no communications access let alone the time required to set their respective records straight.

Background

On January 30, 1967, the Secretary of Defense issued a memorandum directing the use of SSNs in lieu of service member identification numbers.[7] At the time, this was a decision that sought to increase bureaucratic efficiencies particularly from an interagency perspective. For example, the DoD could easily share service member accounting data with the IRS and the Treasury Department, thus eliminating the need for each agency to issue its own, unique identification numbering system. The policy shift to eliminate the need for multiple tracking architectures worked as envisioned and had the added benefit of streamlining accounting processes. On the other hand, these decisions were made long before the advent of the Internet and the profound reduction in barriers to sharing mass amounts of personal and sometimes sensitive information.

[7] "The Social Security Number as a Standard Universal Identifier," *Epic.org, Electronic Privacy Information Center*. <http://www.epic.org/privacy/hew1973 report/c7.htm> (15 November 2005).

Current strategies

Congress and the Bush administration recently acted against the identity theft threat through the Identity Theft Penalty Enhancement Act signed into law on July 15, 2004. This law stiffens legal penalties for those convicted of “aggravated identity theft” and outlines standards of conduct for individuals that work in industries and government agencies responsible for handling personal information.[8]

The DoD has also assumed a strong defensive posture against the identity theft threat through new policy initiatives and an aggressive education campaign. For example, the DoD has eliminated paper copies of leave and earnings statements, initiated strict controls over personal information posted to government web sites, and has combined efforts with the Federal Trade Commission in launching the Military Sentinel, an on-line forum for military personnel and DoD civilians to report identity theft and other consumer frauds.[9] While these actions represent prudent initial steps in addressing the issue of identity theft and more specifically, its impact on service members, these measures fall far short of the dramatic shift in policy required to combat the problem over the long-term. The

[8] Office of the Press Secretary, “President Bush Signs Identity Theft Penalty Enforcement Act,” *The White House.* July 2004, <http://www.whitehouse.gov /news/releases/2004/07/20040715-3.html> (14 November 2004).

[9] Miles, 1.

de-coupling of SSNs as service member identification numbers must be initiated if a dramatic reduction in the identity theft threat is to be realized.

Once the decision has been made to initiate the use of a service member identification number in lieu of the Social Security Number, a DoD task force must be created to understand the full depth and scope of the conversion. This analysis will likely focus on the external agencies affected by the change such as the IRS, the Treasury Department, and the Social Security Administration to name only a few.

A DoD internal review must also be initiated. For instance, it is clear that an organization like the Defense Finance and Accounting Service (DFAS), which relies heavily on the use of SSNs for its finance and accounting mission, would be significantly impacted by any conversion. However, a vast number of agencies or activities within the DoD would also be similarly affected. The Defense Manpower Data Center, the Army and Air Force Exchange Service, the Defense Security Service, and the Tricare Management Activity are only a few examples of other agencies that would be impacted.[10]

[10] "Information System Security: Controls Over the Use and Protection of Social Security Numbers Within the DoD," *Office of the Inspector General of the Department of Defense*, 21 March 2003,

Finally, the task force must examine the information technology (IT) implications of this change, which may well prove to be both time-consuming and costly. Most DoD agencies rely heavily on IT solutions to manage personnel-related tasks and functions. To further complicate matters, many of these systems were specifically designed by the private sector to address functions or tasks unique to that agency. In short, finding a single IT solution that converts all DoD systems to a new identification system will be difficult if not impossible.

Once a thorough review has been completed and its recommendations accepted by the Secretary of Defense, each agency will be responsible for implementing an organization-specific conversion plan and overseeing its progress. Overall agency oversight could be established within the DoD's Office of the Inspector General or through an independent commission established by the Secretary.

Counterarguments

Some may assert that a change of this scope and magnitude is too costly and manpower intensive to be undertaken when balanced against the same criteria associated with the identity

<http://www.dodig.osd.mil/audit/reports/fy03/03066sum.htm. (5 November 2005).

theft threat. This argument is convincingly countered when the very nature of the threat is considered. The force protection vulnerability represented by identity theft will only grow as mass amounts of data continue to be propagated via the Internet and as the technical means of retrieving and exploiting that data becomes more accessible to criminals. As a result, the number of Americans that fall prey to identity theft will increase and by extension, the number of military personnel affected will also increase. The financial, man-hour, and readiness costs paid by the DoD over time will exceed similar factors associated with a conversion.

Institutional models for successfully converting SSNs to unique identification numbers are currently available in business, state government, and academia. Some organizations, such as small colleges or universities, have initiated the change while incurring only a modest cost in time and money. Other institutions have undergone the conversion at a cost that is more comparable to that which might be realized by the DoD. In all instances, however, each model must be carefully scrutinized for strategies and solutions that could be templated for a DoD model. For example, the University of Oregon recently initiated a three to five-year plan for a one-time conversion to unique identification numbers at an estimated cost of $90,000.[11] Of course, with a current student population of 20,339,[12] the scope of this change is hardly comparable to what would be required by the DoD. However, the university's phased approach to the conversion that included assignment of unique identification numbers, removal of SSNs from existing systems, and the initiation of a back-up procedure for core officers to locate records based on SSN, could be adopted by individual DoD agencies or activities.

At a scope and cost more comparable to what might be faced by the DoD, the conversion currently being undertaken by the Blue Cross Blue Shield Association (BCBSA) must also be considered. As a healthcare provider for ninety-three million Americans through its forty independent companies,[13] the complexities and cost of a national conversion plan would be broadly comparable to any DoD proposal. For example, the plan set forth by the BCBSA of Michigan mandates the re-issuance of identification cards and the "re-programming [of] multiple claims and membership systems to accept the new random numbers"

[11] Sue Eveland, "The Numbers Game: Phasing in Generated ID Numbers at the University of Oregon," *PACRAO – Pacific American Association of College Registrars and Admission Officers.* <http://www.pacrao.org/docs/resources/writersteam/StrategiesConvertingSSNs.doc> (14 November 2005).

[12] "About the UO," *University of Oregon.* <http://www.uoregon.edu/about.shtml> (15 December 2005).

[13] "Newsroom: A Reporter's Guide to the Blue Cross and Blue Shield Association," *Blue Cross and Blue Shield Association,* 2005, <http://www.bcbs.com/index.html> (15 December 2005).

on behalf of four million of its members. The cost associated with this undertaking is estimated to be $19 million. "It is a mammoth project as Social Security Numbers have been used to process health care claims for decades."[14]

Those who might criticize a similar DoD plan as being unnecessary due to the cost in time and money involved balanced against comparable factors associated with the identity theft threat, must examine the BCBSA of Michigan model closely. The cost of the conversion expressed on a per member basis is approximately $4.75. If the DoD were to arrive at a similar cost calculation for each member of the 3.3 million total military force,[15] the immediate implementation of a conversion plan could not be ignored. As was previously noted, ten million Americans (approximately 3.4% of the total population[16]) are affected by identity theft every year. Assuming 3.4% of the total military force population was affected by this threat at an average financial cost of $90,000 for each name used and 600

[14] Helen Stojic, "Blue Cross Blue Shield of Michigan and Blue Care Network to Drop Social Security Numbers From 4 Million ID Cards," *Blue Cross Blue Shield of Michigan,* 15 April 2005, <http://www.bcbsm.com/pr/pr050415b.shtml> (15 December 2005).

[15] "DoD Total Force," *Military Family Resource Center,* 2003 Demographics Report, <http://www.mfrc-dodqol.org/pdffiles/demo2003/Section IDoDTotalForce.pdf> (15 December 2005). The total military force of 3,275,265 consists of Active Duty, Reserve (Ready Reserve, Standby Reserve, and Retired Reserve), Guard members, civilian personnel in support of the DoD, and the DHS's Coast Guard.

[16] "The World Factbook," *The Central Intelligence Agency,* July 2005, <http://www.cia.gov/cia/publications/factbook/rankorder/2119rank.html> (15 December 2005).

hours in time lost, the total adverse impact on personnel readiness can be estimated to be $10 billion and 67.3 million hours.

Conclusion

The force protection threat represented by identity theft is profound and must be aggressively addressed within the DoD. The use of the SSN as a service member identification number represents a significant vulnerability that mandates a reversal of the 1967 decision that implemented the current policy. Any conversion of the current identification system will prove to be both time-intensive and costly. However, these impacts do not exceed the long-term financial, man-hour, and readiness costs that will be paid over time by the DoD and individual service members alike. The sophistication and number of identity thieves is increasing and sensitive data, like the SSN, will continue to put the military at risk as long as the current policy remains unchanged.

Word count: 1874

Bibliography

“About the UO.” *University of Oregon,* 2005. <http://www .uoregon.edu/about.shtml> (15 December 2005).

Bruce, Laura “John Harrison – The Face of Identity Theft.” *Bankrate.com,* 18 August 2004. <http://www.bankrate.com/brm /news/advice/IDTheft/ID-home.asp> (14 November 2005).

“DoD Total Force,” *Military Family Resource Center,* 2003 Demographics Report, <http://www.mfrc-dodqol.org/pdffiles /demo2003/SectionIDoDTotalForce.pdf> (15 December 2005).

Eveland, Sue. “The Numbers Game: Phasing in Generated ID Numbers at the University of Oregon.” *PACRAO – Pacific American Association of College Registrars and Admission Officers.* <http://www.pacrao.org/docs/resources /writersteam/StrategiesConvertingSSNs.doc> (14 November 2005).

Foley, Linda and Jay Foley. “Identity Theft: The Impact 2003. A Comprehensive Study to Understand the Impact of Identity Theft on Known Victims.” *Identity Theft Resource Center,* 2003. <http://idtheftcenter.com/idaftermath.pdf> (14 November 2005).

“Identity Theft Focus of National Consumer Protection Week 2005.” *For the Consumer. Federal Trade Commission,* 7 February 2005. <http://www.ftc.gov/opa/2005/02/ncpw05.htm> (14 November 2005).

“Identity Theft – What It Is And How To Avoid It (LAPA 01-04).” *Naval Inspector General.* <http://www.ig.navy.mil /Intelligence%20and%20Security%20(Identity%20Theft).htm> (14 November 2005).

“Information System Security: Controls Over the Use and Protection of Social Security Numbers Within the DoD.” *Office of the Inspector General of the Department of Defense*, 21 March 2003. < http://www.dodig.osd.mil/audit /reports/fy03/03066sum.htm. (5 November 2005).

Miles, Donna. “Military Takes Steps Against Identity Theft.” *Military Money,* Winter 2004-2005. <http://www.militarymoney.com/money/1101916428> (15 November 2005).

“Newsroom: A Reporter’s Guide to the Blue Cross and Blue Shield Association.” *Blue Cross and Blue Shield Association,* 2005. <http://www.bcbs.com/index.html> (15 December 2005).

Office of the Press Secretary. “President Bush Signs Identity Theft Penalty Enforcement Act.” *The White House,* July 2004, <http://www.whitehouse.gov/news/releases/2004 /07/20040715-3.html> (14 November 2004).

Stojic, Helen “Blue Cross Blue Shield of Michigan and Blue Care Network to Drop Social Security Numbers From 4 Million ID Cards.” *Blue Cross Blue Shield of Michigan,* 15 April 2005. <http://www.bcbsm.com/pr/pr050415b.shtml> (15 December 2005).

Swanda, Mitch. “Protecting Your Personal Top Secret.” *National Military Family Association,* January 2005. <http://www.nmfa.org/site/PageServer?pagename=usaa _article_id_theft> (14 November 2005).

“The Social Security Number as a Standard Universal Identifier.” *Epic.org. Electronic Privacy Information Center*. <http://www.epic.org/privacy/hew1973 report/c7.htm> (15 November 2005).

“The World Factbook.” *The Central Intelligence Agency,* July 2005. <http://www.cia.gov/cia/publications/factbook /rankorder/2119rank.html> (15 December 2005).